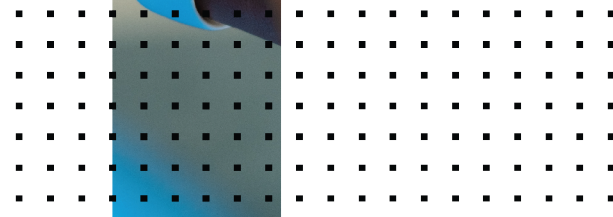
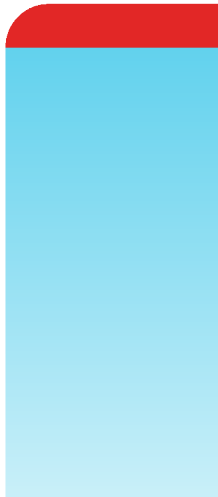


# Release Notes

## FortiManager 7.0.8



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



August 10, 2023

FortiManager 7.0.8 Release Notes

02-708-914606-20230810

# TABLE OF CONTENTS

<b>Change Log</b>	<b>6</b>
<b>FortiManager 7.0.8 Release</b>	<b>7</b>
Supported models	7
FortiManager VM subscription license	7
Management extension applications	7
Supported models for MEA	8
Minimum system requirements	8
<b>Special Notices</b>	<b>10</b>
FortiManager fails to retrieve FortiGate's configuration when external-resource objects include a "g-" prefix	10
FortiManager creates faulty dynamic mapping for VPN manager interface during PP import	10
FAP-831F not yet supported by AP Manager	11
Installing policy packages with 80K rules	11
Authorizing FortiGate with FortiClient EMS connected	11
View Mode is disabled in policies when policy blocks are used	11
FortiManager upgrades from 7.0.0	11
Fortinet verified publisher docker image	11
Scheduling firmware upgrades for managed devices	13
Modifying the interface status with the CLI	13
SD-WAN with upgrade to 7.0	13
Citrix XenServer default limits and upgrade	14
Multi-step firmware upgrades	14
Hyper-V FortiManager-VM running on an AMD CPU	14
SSLv3 on FortiManager-VM64-AWS	14
<b>Upgrade Information</b>	<b>16</b>
Downgrading to previous firmware versions	16
Firmware image checksums	17
FortiManager VM firmware	17
SNMP MIB files	18
<b>Product Integration and Support</b>	<b>19</b>
Supported software	19
Web browsers	20
FortiOS and FortiOS Carrier	20
FortiADC	20
FortiAnalyzer	20
FortiAuthenticator	20
FortiCache	21
FortiClient	21
FortiDDoS	21
FortiDeceptor	21
FortiFirewall and FortiFirewallCarrier	21

FortiMail .....	21
FortiProxy .....	22
FortiSandbox .....	22
FortiSOAR .....	22
FortiSwitch ATCA .....	22
FortiTester .....	23
FortiWeb .....	23
Virtualization .....	23
Feature support .....	23
Language support .....	24
Supported models .....	25
FortiGate models .....	26
FortiGate special branch models .....	28
FortiCarrier models .....	32
FortiCarrier special branch models .....	33
FortiADC models .....	35
FortiAnalyzer models .....	35
FortiAuthenticator models .....	36
FortiCache models .....	36
FortiDDoS models .....	36
FortiDeceptor models .....	36
FortiFirewall models .....	37
FortiFirewallCarrier models .....	37
FortiMail models .....	38
FortiProxy models .....	38
FortiSandbox models .....	38
FortiSOAR models .....	39
FortiSwitch ATCA models .....	39
FortiTester models .....	39
FortiWeb models .....	40
<b>Resolved Issues .....</b>	<b>41</b>
AP Manager .....	41
Device Manager .....	41
Global ADOM .....	42
Others .....	42
Policy and Objects .....	42
System Settings .....	43
VPN Manager .....	43
<b>Known Issues .....</b>	<b>44</b>
Device Manager .....	44
FortiSwitch Manager .....	44
Others .....	44
Policy & Objects .....	45
Script .....	46
System Settings .....	46
VPN Manager .....	46

---

<b>Appendix A - FortiGuard Distribution Servers (FDS)</b>	<b>48</b>
FortiGuard Center update support	48
<b>Appendix B - Default and maximum number of ADOMs supported</b>	<b>49</b>
Hardware models	49
Virtual Machines	49

# Change Log

Date	Change Description
2023-06-08	Initial release.
2023-06-19	Updated <a href="#">Resolved Issues on page 41</a> .
2023-06-23	Updated <a href="#">Special Notices on page 10</a> and <a href="#">Known Issues on page 44</a> .
2023-06-26	Updated <a href="#">FortiOS and FortiOS Carrier on page 20</a> and <a href="#">Known Issues on page 44</a> .
2023-07-04	Updated <a href="#">Resolved Issues on page 41</a> .
2023-07-12	Updated <a href="#">Special Notices on page 10</a> and <a href="#">Known Issues on page 44</a> .
2023-07-19	Updated <a href="#">Web browsers on page 20</a> .
2023-08-04	Updated <a href="#">Known Issues on page 44</a> .
2023-08-10	Updated <a href="#">Known Issues on page 44</a> .

# FortiManager 7.0.8 Release

This document provides information about FortiManager version 7.0.8 build 0452.



The recommended minimum screen resolution for the FortiManager GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

- [Supported models on page 7](#)
- [FortiManager VM subscription license on page 7](#)
- [Management extension applications on page 7](#)

## Supported models

FortiManager version 7.0.8 supports the following models:

<b>FortiManager</b>	FMG-200F, FMG-200G, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, and FMG-3900E.
<b>FortiManager VM</b>	FMG_DOCKER, FMG-VM64, FMG_VM64_ALI, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-IBM, FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

## FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see [FortiManager VM firmware on page 17](#).

See also [Appendix B - Default and maximum number of ADOMs supported on page 49](#).

## Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 7.0.8.



FortiManager uses port TCP/443 or TCP/4443 to connect to the Fortinet registry and download MEAs. Ensure that the port is also open on any upstream FortiGates. For more information about incoming and outgoing ports, see the [FortiManager 7.0 Ports Guide](#).

## Supported models for MEA

You can use any of the following FortiManager models as a host for management extension applications:

<b>FortiManager</b>	FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, and FMG-3900E.
<b>FortiManager VM</b>	FMG_DOCKER, FMG-VM64, FMG_VM64_ALI, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-IBM, FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

## Minimum system requirements

By default FortiManager VMs use the following system resource settings:

- 4 vCPU
- 8 GB RAM
- 500 GB disk space

Starting with FortiManager 7.0.0, RAM and CPU is capped at 50% for MEAs. (Use the `config system docker` command to view the setting.) If FortiManager has 8 CPUs and 16 GB RAM, then only 4 CPUs and 8 GB RAM are available to MEAs by default, and the 4 CPUs and 8 GB RAM are used for all enabled MEAs.

Some management extension applications have minimum system requirements that require you to increase system resources. The following table identifies the minimum requirements for each MEA as well as the recommended system resources to function well in a production environment.

MEA minimum system requirements apply only to the individual MEA and do not take into consideration any system requirements for resource-sensitive FortiManager features or multiple, enabled MEAs. If you are using multiple MEAs, you must increase the system resources to meet the cumulative need of each MEA.

Management Extension Application	Minimum system requirements	Recommended system resources for production*
<b>FortiAIOps</b>	<ul style="list-style-type: none"> <li>• 8 vCPU</li> <li>• 32 GB RAM</li> <li>• 500 GB disk storage</li> </ul>	No change
<b>FortiPortal</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	No change
<b>FortiSigConverter</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	No change
<b>FortiSOAR</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> </ul>	<ul style="list-style-type: none"> <li>• 16 vCPU</li> </ul>



Management Extension Application	Minimum system requirements	Recommended system resources for production*
	<ul style="list-style-type: none"> <li>• 8 GB RAM</li> <li>• 500 GB disk storage</li> </ul>	<ul style="list-style-type: none"> <li>• 64 GB RAM</li> <li>• No change for disk storage</li> </ul>
<b>Policy Analyzer</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	No change
<b>SD-WAN Orchestrator</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 12 GB RAM</li> </ul>
<b>Universal Connector</b>	<ul style="list-style-type: none"> <li>• 1 GHZ vCPU</li> <li>• 2 GB RAM</li> <li>• 1 GB disk storage</li> </ul>	No change
<b>Wireless Manager (FortiWLM)</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	No change

\*The numbers in the *Recommended system resources for production* column are a combination of the default system resource settings for FortiManager plus the minimum system requirements for the MEA.

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.0.8.

## FortiManager fails to retrieve FortiGate's configuration when external-resource objects include a "g-" prefix

**Scenario:** Multi-VDOM is enabled on FGTs version 6.4 and external-resource objects are created globally; these objects are being used in webfilter and firewall policies. After upgrading the FGTs to v7.0, the FGTs automatically add a "g-" prefix to the global external-resource. However, FMG has not supported this prefix yet, so FMG fails to retrieve FGT's configuration to DB.

**Workaround:** There are two workarounds; use the approach that works best for your environment. If it is possible, create a new backup of your FMG and FGT(s) before making any changes.

First workaround approach:

1. Re-create all threat feeds locally in VDOM configuration and update policies and security profiles that reference them to the local threat feed vs. the global feed.
2. Delete the global threat feed objects.

Second workaround approach:

1. Perform policy reinstallation. FMG adds original threat feed objects within the VDOM configuration without the 'g' prefix.
2. FMG reports 'install OK/verify FAIL' at the end of the policy installation.
3. Run scripts to delete the global threat feed objects (objects with the 'g' prefix) from the FGT.
4. Retrieve the FGT configuration from FMG.
5. Perform another policy installation to update the configuration synchronization status between the FGT and FMG. No commands are pushed during this stage according to the install wizard.

## FortiManager creates faulty dynamic mapping for VPN manager interface during PP import

If policy changes are made directly on the FortiGates, the subsequent PP import creates faulty dynamic mappings for VPN manager.

It is strongly recommended to create a fresh backup of the FortiManager's configuration prior to this workaround. Perform the following command to check & repair the FortiManager's configuration database:

```
diagnose cdb check policy-packages <adom>
```

After executing this command, FortiManager will remove the invalid mappings of vpnmgr interfaces.

## FAP-831F not yet supported by AP Manager

The AP Manager module does not yet support the FAP-831F model.

## Installing policy packages with 80K rules

A minimum of 32 GB of memory is required on FortiManager to support the installation of 80K rules to managed FortiGates.

## Authorizing FortiGate with FortiClient EMS connected

Please follow the steps below when managing FortiClient EMS Connector's configuration via FortiManager:

1. Add a FortiGate device to FortiManager.
2. Create FortiClient EMS Connector's configuration on FortiManager.
3. Install the configuration onto the FortiGate device.

If the order of the steps is not followed, FortiClient EMS may not authorize the FortiGate device.

## View Mode is disabled in policies when policy blocks are used

When policy blocks are added to a policy package, the *View Mode* option is no longer available, and policies in the table cannot be arranged by *Interface Pair View*. This occurs because policy blocks typically contain multiple policies using different incoming and outgoing interfaces, however, *View Mode* is still disabled even when policy blocks respect the interface pair.

## FortiManager upgrades from 7.0.0

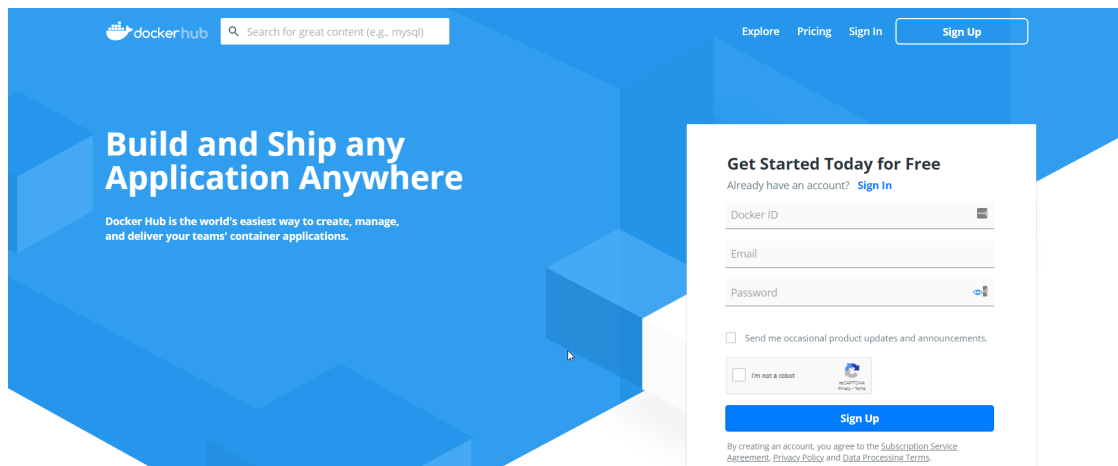
When upgrading from FortiManager 7.0.0, you must first upgrade to 7.0.1 before going to 7.0.2 and later. This is required to correct an issue that causes FortiManager to download unnecessary objects from FortiGuard. Please contact [FortiManager support](#) for more information if required.

## Fortinet verified publisher docker image

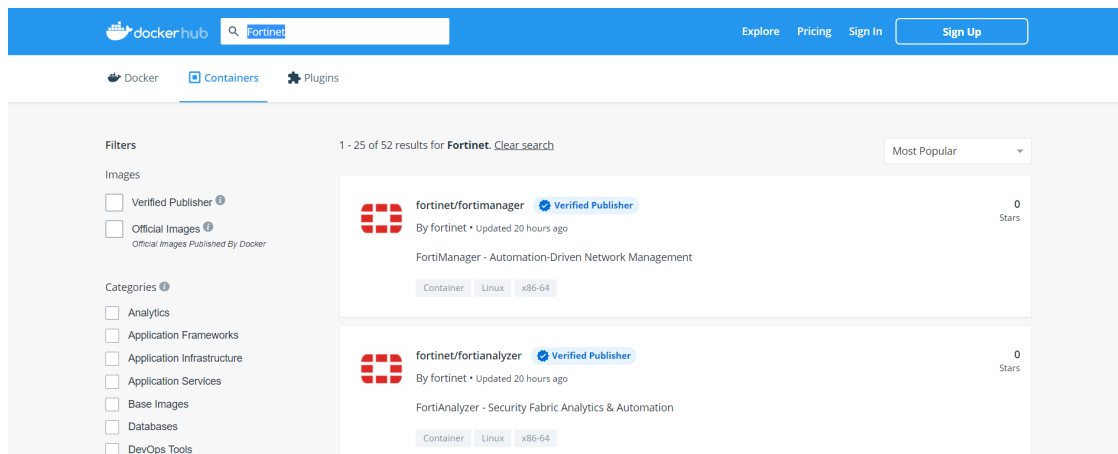
FortiManager docker images are available for download from Fortinet's Verified Publisher public repository on [dockerhub](#).

**To download the FortiManager image from dockerhub:**

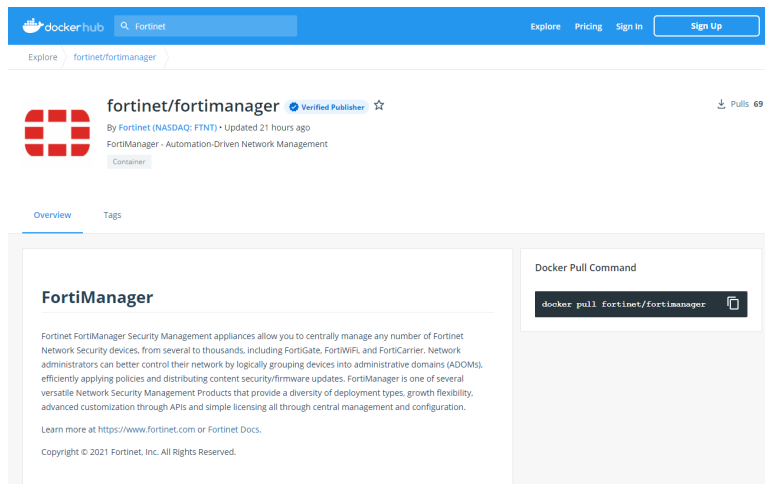
1. Go to dockerhub at <https://hub.docker.com/>.  
The dockerhub home page is displayed.



2. In the banner, click *Explore*.
3. In the search box, type *Fortinet*, and press *Enter*.  
The *fortinet/fortimanager* and *fortinet/fortianalyzer* options are displayed.



4. Click *fortinet/fortimanager*.  
The *fortinet/fortimanager* page is displayed, and two tabs are available: *Overview* and *Tags*. The *Overview* tab is selected by default.



5. On the **Overview** tab, copy the docker pull command, and use it to download the image. The CLI command from the **Overview** tab points to the latest available image. Use the **Tags** tab to access different versions when available.

## Scheduling firmware upgrades for managed devices

Starting in FortiManager 7.0.0, firmware templates should be used to schedule firmware upgrades on managed FortiGates. Attempting firmware upgrade from the FortiManager GUI by using legacy methods may ignore the *schedule upgrade* option and result in FortiGates being upgraded immediately.

## Modifying the interface status with the CLI

Starting in version 7.0.1, the CLI to modify the interface status has been changed from `up/down` to `enable/disable`.

For example:

```
config system interface
  edit port2
    set status <enable/disable>
  next
end
```

## SD-WAN with upgrade to 7.0

Due to design change with SD-WAN Template, upgrading to FortiManager 7.0 may be unable to maintain dynamic mappings for all SD-WAN interface members. Please reconfigure all the missing interface mappings after upgrade.

## Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FMG-VM64-XEN image is larger than 128M. Before updating to FortiManager 6.4, increase the size of the ramdisk setting on Citrix XenServer.

### To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:  

```
xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
```
2. Confirm the setting is in effect by running `xenstore-ls`.  

```
-----  
limits = ""  
pv-kernel-max-size = "33554432"  
pv-ramdisk-max-size = "536,870,912"  
boot-time = ""  
-----
```
3. Remove the pending files left in `/run/xen/pygrub`.



The ramdisk setting returns to the default value after rebooting.

---

## Multi-step firmware upgrades

Prior to using the FortiManager to push a multi-step firmware upgrade, confirm the upgrade path matches the path outlined on our support site. To confirm the path, please run:

```
dia fwmanager show-dev-upgrade-path <device name> <target firmware>
```

Alternatively, you can push one firmware step at a time.

## Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

## SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global  
set ssl-protocol tlsv1
```

end

# Upgrade Information



Prior to upgrading your FortiManager, please review the FortiManager Upgrade Guide in detail as it includes all of the necessary steps and associated details required to upgrade your FortiManager device or VM.

See [FortiManager 7.0.8 Upgrade Guide](#).

You can upgrade to FortiManager 7.0.8 from the following versions:

- FortiManager 6.4.0 to 6.4.x
- FortiManager 7.0.1 to 7.0.x

See also [FortiManager upgrades from 7.0.0 on page 11](#).



Before upgrading FortiManager, check ADOM versions. Check the ADOM versions supported by the destination firmware and the current firmware. If the current firmware uses ADOM versions not supported by the destination firmware, upgrade ADOM versions in FortiManager before upgrading FortiManager to the destination firmware version.

For example, FortiManager 6.4 supports ADOM versions 6.0, 6.2, and 6.4, but FortiManager 7.0 supports ADOM versions 6.2, 6.4, and 7.0. Before you upgrade FortiManager 6.4 to 7.0, ensure that all ADOM 6.0 versions have been upgraded to ADOM version 6.2 or later. See [FortiManager 7.0.8 Upgrade Guide](#).

This section contains the following topics:

- [Downgrading to previous firmware versions on page 16](#)
- [Firmware image checksums on page 17](#)
- [FortiManager VM firmware on page 17](#)
- [SNMP MIB files on page 18](#)

## Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release by using the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrade process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}  
execute format {disk | disk-ext4 | disk-ext3}
```



## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. After logging in, go to *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

## FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

### Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

### Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

### Google Cloud Platform

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.gcp.zip`: Download the 64-bit package for a new FortiManager VM installation.

### Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

### Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `<product>_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.

### Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `<product>_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.



Microsoft Hyper-V 2016 is supported.

---

### Oracle Private Cloud

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.opc.zip`: Download the 64-bit package for a new FortiManager VM installation.

### VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.



For more information see the [FortiManager Data Sheet](#) available on the Fortinet web site. VM installation guides are available in the [Fortinet Document Library](#).

---

## SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

# Product Integration and Support

This section lists FortiManager 7.0.8 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

- [Supported software on page 19](#)
- [Feature support on page 23](#)
- [Language support on page 24](#)
- [Supported models on page 25](#)

## Supported software

FortiManager 7.0.8 supports the following software:

- [Web browsers on page 20](#)
- [FortiOS and FortiOS Carrier on page 20](#)
- [FortiADC on page 20](#)
- [FortiAnalyzer on page 20](#)
- [FortiAuthenticator on page 20](#)
- [FortiCache on page 21](#)
- [FortiClient on page 21](#)
- [FortiDDoS on page 21](#)
- [FortiDeceptor on page 21](#)
- [FortiFirewall and FortiFirewallCarrier on page 21](#)
- [FortiMail on page 21](#)
- [FortiProxy on page 22](#)
- [FortiSandbox on page 22](#)
- [FortiSOAR on page 22](#)
- [FortiSwitch ATCA on page 22](#)
- [FortiTester on page 23](#)
- [FortiWeb on page 23](#)
- [Virtualization on page 23](#)



To confirm that a device model or firmware version is supported by the current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```



Always review the Release Notes of the supported platform firmware version before upgrading your device.

---

## Web browsers

FortiManager 7.0.8 supports the following web browsers:

- Microsoft Edge 114
- Mozilla Firefox version 101
- Google Chrome version 114

Other web browsers may function correctly, but are not supported by Fortinet.

## FortiOS and FortiOS Carrier



The *FortiManager Release Notes* communicate support for FortiOS versions that are available at the time of the FortiManager 7.0.8 release. For additional information about other supported FortiOS versions, please refer to the FortiManager compatibility chart in the [Fortinet Document Library](#).

See [FortiManager compatibility with FortiOS](#).

---

FortiManager 7.0.8 supports the following versions of FortiOS and FortiOS Carrier:

- 7.0.0 to 7.0.12
- 6.4.0 to 6.4.14
- 6.2.0 to 6.2.15

## FortiADC

FortiManager 7.0.8 supports the following versions of FortiADC:

- 7.0.0 and later
- 6.2.0 and later
- 6.1.0 and later

## FortiAnalyzer

FortiManager 7.0.8 supports the following versions of FortiAnalyzer:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

## FortiAuthenticator

FortiManager 7.0.8 supports the following versions of FortiAuthenticator:

- 6.4.0 and later
- 6.3.0 and later
- 6.2.0 and later

## FortiCache

FortiManager 7.0.8 supports the following versions of FortiCache:

- 4.2.0 and later
- 4.1.0 and later
- 4.0.0 and later

## FortiClient

FortiManager 7.0.8 supports the following versions of FortiClient:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.1 and later

## FortiDDoS

FortiManager 7.0.8 supports the following versions of FortiDDoS:

- 6.3.0 and later
- 6.2.0 and later
- 6.1.0 and later

Limited support. For more information, see [Feature support on page 23](#).

## FortiDeceptor

FortiManager 7.0.8 supports the following versions of FortiDeceptor:

- 4.1 and later
- 4.0 and later
- 3.3 and later

## FortiFirewall and FortiFirewallCarrier

FortiManager 7.0.8 supports the following versions of FortiFirewall and FortiFirewallCarrier:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

## FortiMail

FortiManager 7.0.8 supports the following versions of FortiMail:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

## FortiProxy

FortiManager 7.0.8 supports configuration management for the following versions of FortiProxy:

- 7.0.8
- 7.0.7
- 7.0.6
- 7.0.5



Configuration management support is identified as *Management Features* in these release notes. See [Feature support on page 23](#).

---

FortiManager 7.0.8 supports logs from the following versions of FortiProxy:

- 7.0.0 to 7.0.8
- 2.0.0 to 2.0.5
- 1.2.0 to 1.2.13
- 1.1.0 to 1.1.6
- 1.0.0 to 1.0.7

## FortiSandbox

FortiManager 7.0.8 supports the following versions of FortiSandbox:

- 4.2.0 and later
- 4.0.0 and 4.0.1
- 3.2.0 and later
- 3.1.0 and later

## FortiSOAR

FortiManager 7.0.8 supports the following versions of FortiSOAR:

- 7.0.0 and later
- 6.4.0 and later
- 6.0.0 and later

## FortiSwitch ATCA

FortiManager 7.0.8 supports the following versions of FortiSwitch ATCA:

- 5.2.0 and later
- 5.0.0 and later
- 4.3.0 and later

## FortiTester

FortiManager 7.0.8 supports the following versions of FortiTester:

- 7.0.0 and later
- 4.2.0 and later
- 4.1.0 and later

## FortiWeb

FortiManager 7.0.8 supports the following versions of FortiWeb:

- 7.0.0 and later
- 6.4.0 and later
- 6.3.0 and later

## Virtualization

FortiManager 7.0.8 supports the following virtualization software:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Google Cloud Platform
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012, 2016, and 2019
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- Oracle Private Cloud
- VMware ESXi versions 6.5 and later

## Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiGate	✓	✓	✓	✓	✓

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiCarrier	✓	✓	✓	✓	✓
FortiADC		✓	✓		
FortiAnalyzer			✓	✓	✓
FortiAuthenticator					✓
FortiCache			✓	✓	✓
FortiClient		✓		✓	✓
FortiDDoS			✓	✓	✓
FortiDeceptor		✓			
FortiFirewall	✓				✓
FortiFirewall Carrier	✓				✓
FortiMail		✓	✓	✓	✓
FortiProxy	✓	✓	✓	✓	✓
FortiSandbox		✓	✓	✓	✓
FortiSOAR		✓	✓		
FortiSwitch ATCA	✓				
FortiTester		✓			
FortiWeb		✓	✓	✓	✓
Syslog					✓

## Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Japanese	✓	✓
Korean	✓	✓



Language	GUI	Reports
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings > Admin > Admin Settings*, in *Administrative Settings > Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiManager, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiManager. For more information, see the *FortiManager Administration Guide*.

## Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 7.0.8.



Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

This section contains the following topics:

- [FortiGate models on page 26](#)
- [FortiGate special branch models on page 28](#)
- [FortiCarrier models on page 32](#)
- [FortiCarrier special branch models on page 33](#)
- [FortiADC models on page 35](#)
- [FortiAnalyzer models on page 35](#)
- [FortiAuthenticator models on page 36](#)
- [FortiCache models on page 36](#)
- [FortiDDoS models on page 36](#)
- [FortiDeceptor models on page 36](#)
- [FortiFirewall models on page 37](#)
- [FortiFirewallCarrier models on page 37](#)
- [FortiMail models on page 38](#)
- [FortiProxy models on page 38](#)
- [FortiSandbox models on page 38](#)
- [FortiSOAR models on page 39](#)
- [FortiSwitch ATCA models on page 39](#)
- [FortiTester models on page 39](#)
- [FortiWeb models on page 40](#)

## FortiGate models

The following FortiGate models are released with FortiOS firmware. For information about supported FortiGate models on special branch releases of FortiOS firmware, see [FortiGate special branch models on page 28](#).

Model	Firmware Version
<b>FortiGate:</b> FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60EDSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80E, FortiGate80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-400F, FortiGate-401E, FortiGate-401F, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F <b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 <b>FortiGate DC:</b> FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC <b>FortiGate ACDC:</b> FortiGate-2201E-ACDC, FortiGate-3960E-ACDC <b>FortiWiFi:</b> FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE <b>FortiGate VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGateVM64-Xen, FortiGate-VMX, FortiGate-VMX-Service-Manager, FortiGate-ARM64-AWS, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, <b>FortiOS VM:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen <b>FortiGateRugged:</b> FortiGateRugged-60F, FortiGateRugged-60F-3G4G	7.0

Model	Firmware Version
<b>FortiGate:</b> FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-80F-POE, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F	6.4
<b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	
<b>FortiGate DC:</b> FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC	
<b>FortiGate ACDC:</b> FortiGate-2201E-ACDC, FortiGate-3960E-ACDC	
<b>FortiGate Hardware Low Encryption:</b> FortiGate-100D-LENC	
<b>FortiWiFi:</b> FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F,	
<b>FortiGate VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen, FortiGate-VMX, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM	
<b>FortiOS VM:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
<b>FortiGateRugged:</b> FortiGateRugged-60F, FortiGateRugged-60F-3G4G	

Model	Firmware Version
<b>FortiGate:</b> FortiGate-30E, FortiGate-30E-3G4G-GBL, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FG-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FG-400E, FG-400E-Bypass, FG-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000C, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E <b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 <b>FortiGate DC:</b> FortiGate-80C-DC, FortiGate-401E-DC, FortiGate-600C-DC, FortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC <b>FortiGate Hardware Low Encryption:</b> FortiGate-80C-LENC, FortiGate-100D-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC <b>FortiWiFi:</b> FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-81F-2R-POE, <b>FortiGate-VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager <b>FortiOS:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen <b>FortiGate Rugged:</b> FortiGateRugged-30D, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-90D	6.2

## FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.0.8 supports these models on the identified FortiOS version and build number.

For information about supported FortiGate models released with FortiOS firmware, see [FortiGate models on page 26](#).

## FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80F-DSL	7.0.11	4974
FortiGate-900G	7.0.10	6566
FortiGate-901G		
FortiGate-1000F	7.0.12	6660
FortiGate-1001F		
FortiGate-1500G	7.0.9	6458
FortiGate-1501G		
FortiGate-3200F	7.0.12	6661
FortiGate-3201F		
FortiGate-3700F	7.0.12	6661
FortiGate-3701F		
FortiGate-4800F	7.0.12	6661
FortiGate-4801F		
FortiGate-6000F	7.0.12	0163
FortiGate-6300F		
FortiGate-6300F-DC		
FortiGate-6301F		
FortiGate-6301F-DC		
FortiGate-6500F		
FortiGate-6500F-DC		
FortiGate-6501F		
FortiGate-6501F-DC		
FortiGate-7000E	7.0.12	0163
FortiGate-7030E		
FortiGate-7040E		
FortiGate-7060E		
FortiGate-7060E-8-DC		
FortiGate-7000F	7.0.12	0163
FortiGate-7081F		
FortiGate-7121F		
FortiGate-7121F-2		
FortiGate-7121F-2-DC		
FortiGate-7121F-DC		
FortiGateRugged-70F	7.0.11	6565
FortiGateRugged-70F-3G4G		

## FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-400F	6.4.12	5429
FortiGate-401F		
FortiGate-600F	6.4.12	5429
FortiGate-601F		
FortiWiFi-80F-2R	6.4.8	5033
FortiWiFi-81F-2R		
FortiWiFi-81F-2R-3G4G-POE		
FortiWiFi-81F-2R-POE		
FortiWiFi-80F-2R-3G4G-DSL		
FortiGate-3500F	6.4.6	5886
FortiGate-3501F	6.4.6	6132
FortiGate-6000F	6.4.13	1926
FortiGate-6300F		
FortiGate-6300F-DC		
FortiGate-6301F		
FortiGate-6301F-DC		
FortiGate-6500F		
FortiGate-6500F-DC		
FortiGate-6501F		
FortiGate-6501F-DC		
FortiGate-7000E	6.4.13	1926
FortiGate-7030E		
FortiGate-7040E		
FortiGate-7060E		
FortiGate-7060E-8-DC		
FortiGate-7000F	6.4.13	1926
FortiGate-7081F		
FortiGate-7121F		
FortiGate-7121F-2		
FortiGate-7121F-2-DC		
FortiGate-7121F-DC		

## FortiOS 6.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80D	6.2.13	5238
FortiGate-200F, FortiGate-201F	6.2.13	7249
FortiGate-1800F, FortiGate-1800F-DC FortiGate-1801F, FortiGate-1801F-DC	6.2.9	7197
FortiGate-2600F, FortiGate-2600F-DC FortiGate-2601F, FortiGate-2601F-DC	6.2.9	7197
FortiGate-4200F, FortiGate-4200F-DC FortiGate-4201F, FortiGate-4201F-DC	6.2.9	7197
FortiGate-4400F, FortiGate-4400F-DC	6.2.9	7197
FortiGate-4401F, FortiGate-4401F-DC	6.2.9	7197
FortiGate-6000F FortiGate-6300F FortiGate-6300F-DC FortiGate-6301F FortiGate-6301F-DC FortiGate-6500F FortiGate-6500F-DC FortiGate-6501F FortiGate-6501F-DC	6.2.13	1271
FortiGate-7000E FortiGate-7030E FortiGate-7040E FortiGate-7060E FortiGate-7060E-8-DC	6.2.13	1271
FortiGate-7000F FortiGate-7081F FortiGate-7121F FortiGate-7121F-2 FortiGate-7121F-2-DC FortiGate-7121F-DC	6.2.13	1271
FortiWiFi-80F-2R-3G4G-DSL FortiWiFi-81F-2R-3G4G-DSL	6.2.6	7219
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099

## FortiCarrier models

Model	Firmware Version
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4400F-DC, FortiCarrier-4400F-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen, FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI	7.0
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4400F-DC, FortiCarrier-4400F-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC <b>FortiCarrier 6K and 7K:</b> FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7000F, FortiCarrier-7121F, FortiCarrier-7121F-2	6.2



Model	Firmware Version
<b>FortiCarrier 6K and 7K DC:</b> FortiCarrier-6000F-DC, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC, FortiCarrier-7060E-8-DC, FortiCarrier-7121F-DC, FortiCarrier-7121F-2-DC <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	

## FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 7.0.8 supports these models on the identified FortiOS Carrier version and build number.

For information about supported FortiCarrier models released with FortiOS Carrier firmware, see [FortiCarrier models on page 32](#).

### FortiCarrier 7.0

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3200F FortiCarrier-3201F	7.0.12	6661
FortiCarrier-3700F FortiCarrier-3701F	7.0.12	6661
FortiCarrier-4800F FortiCarrier-4801F	7.0.12	6661
FortiCarrier-6000F FortiCarrier-6300F FortiCarrier-6300F-DC FortiCarrier-6301F FortiCarrier-6301F-DC FortiCarrier-6500F FortiCarrier-6500F-DC FortiCarrier-65001F FortiCarrier-6501F-DC	7.0.12	0163
FortiCarrier-7000E FortiCarrier-7030E FortiCarrier-7040E FortiCarrier-7060E FortiCarrier-7060E-8-DC	7.0.12	0163
FortiCarrier-7000F	7.0.12	0163

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-7081F		
FortiCarrier-7121F		
FortiCarrier-7121F-DC		
FortiCarrier-7121F-2		
FortiCarrier-7121F-2-DC		

## FortiCarrier 6.4

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3500F	6.4.6	5886
FortiCarrier-3501F	6.4.6	6132
FortiCarrier-6000F	6.4.13	1926
FortiCarrier-6300F		
FortiCarrier-6300F-DC		
FortiCarrier-6301F		
FortiCarrier-6301F-DC		
FortiCarrier-6500F		
FortiCarrier-6500F-DC		
FortiCarrier-65001F		
FortiCarrier-6501F-DC		
FortiCarrier-7000E	6.4.13	1926
FortiCarrier-7030E		
FortiCarrier-7040E		
FortiCarrier-7060E		
FortiCarrier-7060E-8-DC		
FortiCarrier-7000F	6.4.13	1926
FortiCarrier-7081F		
FortiCarrier-7121F		
FortiCarrier-7121F-DC		
FortiCarrier-7121F-2		
FortiCarrier-7121F-2-DC		

## FortiADC models

Model	Firmware Version
<b>FortiADC:</b> FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F <b>FortiADC VM:</b> FortiADC-VM	6.2, 7.0
<b>FortiADC:</b> FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F <b>FortiADC VM:</b> FortiADC-VM	6.0, 6.1

## FortiAnalyzer models

Model	Firmware Version
<b>FortiAnalyzer:</b> FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E <b>FortiAnalyzer VM:</b> FortiAnalyzer-DOCKER, FortiAnalyzer-VM64, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.0
<b>FortiAnalyzer:</b> FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E <b>FortiAnalyzer VM:</b> FortiAnalyzer-DOCKER, FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	6.4
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-200F, FAZ-300D, FAZ-300F, FAZ-300G, FAZ-400E, FAZ-800F, FAZ-1000D, FAZ-1000E, FAZ-1000F, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3000G, FAZ-3500E, FAZ-3500F, FAZ-3500G, FAZ-3700F and FAZ-3900E. <b>FortiAnalyzer VM:</b> FortiAnalyzer-DOCKER, FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.2

## FortiAuthenticator models

Model	Firmware Version
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E <b>FortiAuthenticator VM:</b> FAC-VM	6.2, 6.3, 6.4

## FortiCache models

Model	Firmware Version
<b>FortiCache:</b> FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E <b>FortiCache VM:</b> FCH-KVM, FCH-VM64	4.1, 4.2
<b>FortiCache:</b> FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E <b>FortiCache VM:</b> FCH-VM64	4.0

## FortiDDoS models

Model	Firmware Version
<b>FortiDDoS:</b> FortiDDoS-2000F	6.3
<b>FortiDDoS:</b> FortiDDoS-200F, FortiDDoS-1500F <b>FortiDDoS VM:</b> FortiDDoS-VM	6.1, 6.2, 6.3

## FortiDeceptor models

Model	Firmware Version
<b>FortiDeceptor:</b> FDC-1000F, FDC-1000G <b>FortiDeceptor Rugged:</b> FDCR-100G <b>FortiDeceptor VM:</b> FDC-VM	4.1
<b>FortiDeceptor:</b> FDC-1000F, FDC-1000G <b>FortiDeceptor Rugged:</b> FDCR-100G <b>FortiDeceptor VM:</b> FDC-VM	4.0
<b>FortiDeceptor:</b> FDC-1000F, FDC-3000D <b>FortiDeceptor VM:</b> FDC-VM	3.3

## FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.0.8 supports these models on the identified FortiFirewall firmware version and build number.

Model	Firmware Version	Firmware Build
<b>FortiFirewall:</b> FortiFirewall-3001F	7.0	4955
<b>FortiFirewall:</b> FortiFirewall-3501F	7.0	4940
<b>FortiFirewall:</b> FortiFirewall-3980E <b>FortiFirewall DC:</b> FortiFirewall-3980E-DC	7.0	487
<b>FortiFirewall VM:</b> FortiFirewall-VM64	7.0	486
<b>FortiFirewall:</b> FortiFirewall-3980E, FortiFirewall-4200F, FortiFirewall-4400F <b>FortiFirewall DC:</b> FortiFirewall-3980E-DC <b>FortiFirewall VM:</b> FortiFirewall-VM64, FortiFirewall-VM64-KVM	6.4	1999
<b>FortiFirewall:</b> FortiFirewall-4401F <b>FortiFirewall DC:</b> FortiFirewall-4401F-DC	6.4	5423
<b>FortiFirewall:</b> FortiFirewall-2600F <b>FortiFirewall DC:</b> FortiFirewall-2600F-DC	6.4	5423
<b>FortiFirewall:</b> FortiFirewall-1801F <b>FortiFirewall DC:</b> FortiFirewall-1801F-DC	6.4	5423
<b>FortiFirewall:</b> FortiFirewall-3980E <b>FortiFirewall DC:</b> FortiFirewall-3980E-DC	6.2	1262
<b>FortiFirewall:</b> FortiFirewall-4200F	6.2.7	5141
<b>FortiFirewall:</b> FortiFirewall-4400F	6.2.7	5148

## FortiFirewallCarrier models

The following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.0.8 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version	Firmware Build
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-3001F	7.0	4955
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-3501F	7.0	4940
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.4	1999

Model	Firmware Version	Firmware Build
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4401F	6.4	5423
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.2.7	5148

## FortiMail models

Model	Firmware Version
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E <b>FortiMail VM:</b> FML-VM	7.0
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E <b>FortiMail VM:</b> FML-VM	6.2, 6.4

## FortiProxy models

Model	Firmware Version
<b>FortiProxy:</b> FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G <b>FortiProxy VM:</b> FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.0
<b>FortiProxy:</b> FPX-400E, FPX-2000E, FPX-4000E <b>FortiProxy VM:</b> FortiProxy-KVM, FortiProxy-VM64	1.2, 2.0

## FortiSandbox models

Model	Firmware Version
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D <b>FortiSandbox DC:</b> FSA-1000F-DC <b>FortiSandbox-VM:</b> FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	4.0, 4.2
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox DC:</b> FSA-1000F-DC <b>FortiSandbox-VM:</b> FortiSandbox-AWS, FSA-VM	3.1, 3.2

## FortiSOAR models

Model	Firmware Version
<b>FortiSOAR VM:</b> FortiSOAR-VM	6.0, 6.4, 7.0

## FortiSwitch ATCA models

Model	Firmware Version
<b>FortiController:</b> FTCL-5103B, FTCL-5903C, FTCL-5913C	5.2
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B <b>FortiController:</b> FTCL-5103B	5.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B	4.3

## FortiTester models

Model	Firmware Version
<b>FortiTester:</b> FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F <b>FortiTester VM:</b> FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.0
<b>FortiTester:</b> FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F <b>FortiTester VM:</b> FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	4.2
<b>FortiTester:</b> FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F <b>FortiTester VM:</b> FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	4.1

## FortiWeb models

Model	Firmware Version
<b>FortiWeb:</b> FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-2000F, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3000F, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E, FortiWeb-4000F <b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.4, 7.0
<b>FortiWeb:</b> FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E <b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.3



# Resolved Issues

The following issues have been fixed in 7.0.8. To inquire about a particular bug, please contact [Customer Service & Support](#).

## AP Manager

Bug ID	Description
767774	Installation failed as FortiManager attempts to change <code>power-level</code> and <code>power-value</code> under the <code>wireless-controller</code> settings at the same time.
781561	User may not be able to access <i>AP Manager</i> with custom read only admin profile.
861941	FortiManager attempts to install " <code>arp-profile</code> " even if " <code>darp</code> " is disabled.

## Device Manager

Bug ID	Description
803425	Installation failed due to the some of the "os-check-list" items which are not supported by the FortiGates anymore.
836933	Changes on the External-Resource settings from ADOMs for specific VDOMs/FGTs alter the External-Resource settings for other ADOMs and VDOMs.
838462	Adding device using " <i>Add Model HA Cluster</i> " feature failed as FortiManager does not allow "virtual switch interfaces" being used as "heartbeat interfaces".
864588	<i>Firmware Template</i> under the <i>Device Manager</i> does not work properly; It might display "No Device".
876040	Status of Certificates is displayed as "pending" under the System's Certificates.
891341	Installation fails due to the Copy failure error; system template created with some empty string values which are assigned to devices.
896998	Unable to get access to the Certificates via <i>Device Manager</i> > <i>DEVICE_NAME</i> > <i>VDOM_NAME</i> > <i>System</i> .
897863	After deselecting the ' <code>allow-dns</code> ' feature under the application control list, the changes cannot be saved.
898814	FortiManager keeps changing the <code>cert-id-validation</code> 's value to its default value during the installation.

Bug ID	Description
902316	Unable to delete unused Template Groups
909867	FortiManager attempts to configure unsupported syntax for "sdwan health-check".

## Global ADOM

Bug ID	Description
906058	Firewall address cannot be deleted from Global ADOM; it displays an error message indicating that the object is being used in ADOM root.

## Others

Bug ID	Description
851586	FortiManager displays "invalid scope" errors when running the "diagnose cdb check policy-packages" command.
873110	FortiManager displays "expired" instead of "not licensed" for non-purchased FortiGuard services.
897157	Unexpected changes in existing static routes created by static route template after upgrade to 7.0.7, 7.2.2, 7.4.0.
899570	Unable to add the "FortiGateRugged-60F" FGT to the FortiManager.
899750	ADOM upgrade makes the Policy Packages status modified.
919088	GUI may not work properly in Google Chrome and Microsoft Edge version 114.

## Policy and Objects

Bug ID	Description
656991	FortiManager should not allow VIP to be created with same IP for External IP and Mapped IP Address.
798955	Traffic shaping policy changes does not trigger any changes/updates on the Policy Packages status.
866826	Failed to modify Virtual Server addresses in Firewall Policies with Deny Action.
880575	When using the "reinstall policy" option to install to devices with different policy packages, the

Bug ID	Description
	corresponding event log shows the same policy package pushed to all devices.
889068	Unable to push policies when VDOMs are in different ADOMs.
895979	FortiManager attempts setting the Zone as the interface for firewall policy, during the installation.
896491	Installation fails with unclear error message "vdom copy failed".
898334	Policy Package Export to Excel is not working for all policy types.

## System Settings

Bug ID	Description
897945	The configured theme of FortiManager is not displayed prior to logging in.

## VPN Manager

Bug ID	Description
857051	Installing a policy package with IPSec VPN to FortiGates fail with the following error: "TCL error(The remote gateway is a duplicate of another IPsec gateway entry)".

# Known Issues

The following issues have been identified in 7.0.8. To inquire about a particular bug or to report a bug, please contact [Customer Service & Support](#).

## Device Manager

Bug ID	Description
752443	Vertical scroll bar is missing in SD-WAN configuration.
768289	There is a discrepancy in the usage of quotation marks (") when configuring DHCP relay from FortiManager or retrieving it from FortiGate.
895001	The "gui-ztna" configuration is displayed as enabled on the FortiManager even though this setting is disabled on the FortiGate.
899350	Promote button is missing for FortiGate-80F Clusters.
910391	When FortiManager operates in a non-default workspace mode, it may attempt to purge the configuration of the FortiGate devices due to database corruption.
925546	Assigned Devices on Provisioning Template/CLI Template shows incorrect VDOM.

## FortiSwitch Manager

Bug ID	Description
881766	Event logs or task manager do not show which user authorized a Fortiswitch .

## Others

Bug ID	Description
777831	When FortiAnalyzer is added as a managed device to FortiManager, " <i>Incident &amp; Event</i> " Tile will be displayed instead of the " <i>FortiSoC</i> ".
895081	Some FortiGates were unable to be upgraded from FortiManager due to firmware ID discrepancies between FortiManager and FortiGuard.
910175	When provisioning the FortiExtender via CLI template, FortiManager displays the "mismatch

Bug ID	Description
	interface" error message.
916463	The approval emails are not being sent to the "Email Notification" admins when a new session is created and submitted for approval.

## Policy & Objects

Bug ID	Description
751443	<p>FortiManager displays policy installation copy failures error when ipsec template gets unassigned.</p> <p><b>Workaround:</b> Instead of unassigning IPSec template, modify IPSec template, replace the reference to IPSec tunnel interface with another interface. Please ensure a fresh FortiManager backup is created prior to any changes.</p>
793240	<p>FortiManager fails to retrieve FortiGate's configuration when external-resource objects include a "g-" prefix.</p> <p>There are two workarounds; use the approach that works best for your environment. If it is possible, create a new backup of your FMG and FGT(s) before making any changes:</p> <p>First workaround approach:</p> <ol style="list-style-type: none"> <li>1. Re-create all threat feeds locally in VDOM configuration and update policies and security profiles that reference them to the local threat feed vs. the global feed.</li> <li>2. Delete the global threat feed objects.</li> </ol> <p>Second workaround approach:</p> <ol style="list-style-type: none"> <li>1. Perform policy reinstallation. FMG adds original threat feed objects within the VDOM configuration without the 'g' prefix.</li> <li>2. FMG reports 'install OK/verify FAIL' at the end of the policy installation.</li> <li>3. Run scripts to delete the global threat feed objects (objects with the 'g' prefix) from the FGT.</li> <li>4. Retrieve the FGT configuration from FMG.</li> <li>5. Perform another policy installation to update the configuration synchronization status between the FGT and FMG. No commands are pushed during this stage according to the install wizard.</li> </ol>
845022	SDN Connector failed to import objects from VMware VSphere.
851331	Cloning Firewall Addresses under the <i>Firewall Objects</i> does not clone the "Add To Groups" entries.
855073	The "where used" feature does not function properly.
863819	Unable to delete unused objects.
883064	If any admin makes changes to the "Object Selection Pane", whether setting it to "Dock to Right", "Dock to Bottom" or "Classic Dual Pane", it will affect all other admin's GUI preferences.

Bug ID	Description
896461	FortiManager disables <code>ip6-send-adv</code> after opening and closing interface configuration.
898883	Exported firewall policies do not contain firewall address values IP, netmask and other details.
902298	FortiManager does not generate error messages when invalid or obsolete application IDs are used in the policy. Instead, it allows installation and sets the category to <i>'pass'</i> or <i>'monitor'</i> .
911632	When retrieving the configuration from the FortiGate, the FortiManager shows the new cert; however, those cannot be assigned to the FCT EMS connector.
922648	FortiManager unable to push WiFi SSID to FortiGates.
925076	FortiManager tries to install different <code>preconnection-id</code> under <i>VPN SSL WEB Portal &gt; Profile &gt; Bookmark-Group &gt; Gui-Bookmark &gt; Book</i> .

## Script

Bug ID	Description
913360	Device script is trying to add additional configuration; therefore, installation gets failed.

## System Settings

Bug ID	Description
825319	FortiManager fails to promote a FortiGate HA member (running on firmware 7.2.0 to 7.2.4) to the Primary.
853429	Creating FortiManager's configuration backup via scp cannot be done.
861997	Unable to delete a particular non-default empty ADOM.

## VPN Manager

Bug ID	Description
513317	FortiManager may fail to install policy after FortiGate failover on Azure.
784385	<p>If policy changes are made directly on the FortiGates, the subsequent PP import creates faulty dynamic mappings for <i>VPN Manager</i>.</p> <p><b>Workaround:</b> It is strongly recommended to create a fresh backup of the FortiManager's configuration prior to the workaround. Perform the following command to check &amp; repair the FortiManager's configuration database.</p>

Bug ID	Description
	<pre>diagnose cdb check policy-packages &lt;adom&gt;</pre> <p>After running this command, FortiManager will remove the invalid mappings of vpnmgr interfaces.</p>

## Appendix A - FortiGuard Distribution Servers (FDS)

In order for FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as an FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the following items:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default, and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through port 443.

### FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform:

Platform	Update Service	Query Service
FortiGate	✓	✓
FortiADC	✓	
FortiCache	✓	
FortiCarrier	✓	✓
FortiClient	✓	
FortiDeceptor	✓	✓
FortiDDoS	✓	
FortiEMS	✓	
FortiMail	✓	✓
FortiProxy	✓	✓
FortiSandbox	✓	✓
FortiSOAR	✓	
FortiTester	✓	
FortiWeb	✓	



## Appendix B - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiManager hardware models and virtual machines.

### Hardware models

FortiManager supports a default number of ADOMs based on hardware model.

Some hardware models support an ADOM subscription license. When you purchase an ADOM subscription license, you increase the number of supported ADOMs. For example, you can purchase an ADOM subscription license for the FMG-3000G series, which allows you to use up to a maximum of 8000 ADOMs.

Other hardware models do not support the ADOM subscription license. For hardware models that do not support the ADOM subscription license, the default and maximum number of ADOMs is the same.

FortiManager Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
200G Series	30		30
300F Series	100		100
400G Series	150		150
1000F Series	1000		1000
2000E Series	1200		1200
3000G Series	4000	✓	8000
3700G Series	10,000	✓	12,000

For FortiManager F series and earlier, the maximum number of ADOMs is equal to the maximum devices/VDOMs as described in the [FortiManager Data Sheet](#).

### Virtual Machines

FortiManager VM subscription license includes five (5) ADOMs. Additional ADOMs can be purchased with an ADOM subscription license.

For FortiManager VM perpetual license, the maximum number of ADOMs is equal to the maximum number of Devices/VDOMs listed in the [FortiManager Data Sheet](#).



FortiManager VM subscription and perpetual licenses are stackable.

---



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.